TITLE OF THE INVENTION

MANAGEMENT APPARATUS, TERMINAL APPARATUS AND MANAGEMENT SYSTEM

BACKGROUND OF THE INVENTION

(1) Field of the Invention

本発明は個人用コンピュータや情報端末等からなるネットワークにおいて端末装置間で処理されるデータを管理する管理装置及び端末装置に関する。

(2) Description of the Prior Art

近年、複数の端末が接続して構成されるネットワークを利用して、ピアトゥピアと呼ばれるような個人用コンピュータ等の端末間での有料コンテンツファイルや著作権保護が必要な情報を配信する形態が利用されている。この端末間でのコンテンツファイル等のデータのやり取りにおいては、従来のサーバ装置が一意にデータを記録、管理して処理を要求する端末に送信する形態ではなく、コンテンツホルダー等の端末装置と処理を要求する端末装置との間でデータのやり取りが行われる。従って、このような端末間同士での有料情報配信サービスにおいては、購入希望者に対してコンテンツを保持するコンテンツホルダーや著作権管理者が認めた正規の情報のみを配信することが重要になる。

そして、端末間でのデータのやり取りの正当性を管理するためのネットワークバスを介して管理装置を設ける方法が提供されている。図２０は、従来のネットワークを介した管理装置２００１及び端末間におけるデータ管理の全体図を示す。

図２０において、処理依頼端末２００３は、配信を希望するコンテンツファイルが、例えば「music.mp3」であることを管理装置２００１に送信する。管理装置２００１では、取得を希望するファイルの依頼先端末２００２を記載したリストを参照して、要求されたファイル情報「music.mp3」を保持している依頼先端末２００２の検索を行う。そして、管理装置２００１はこの検索結果をネットワークバスを介して、配信要求する処理依頼端末２００３に対して返信する。このことにより、処理依頼端末２００３ではファイル「music.mp3」を保持する依頼先端末

２００２との間でのやり取りを開始することが可能になる。

そして、サーバ装置を介さずに端末から端末に対して正規の情報のみを配信確認する方法の一例として電子すかしと呼ばれる方法もある。この電子すかしによれば、処理される情報本体に影響を与えず、情報の正当性を示す情報を「すかし」として埋め込む。

また、端末装置において登録される情報の種類をチェックして、規定された種類以外の情報の登録を拒否する方法もある（例えば、特開平０７－１０５２９０号公報参照）。この特許文献１においては、設定された帳票データの種類と異なるデータが入力された場合に、その登録を拒否して帳票データの誤入力を的確に阻止することが開示されている。

さらに、コンテンツファイルのやり取りにおいては、認証サーバと呼ばれる装置をネットワーク上に配備し、コンテンツファイルを一意に管理して、サーバ装置側で情報を受信できる権利があるかどうかをユーザ端末毎に判断して、ユーザが取得を希望するコンテンツファイルをサーバ装置から端末側に送信する形態が一般的となっている。

しかしながら、上述した図２０の管理装置を用いた端末間でのデータのやり取りを管理する方法においては、管理装置は配信元となる端末を特定するのみで、ファイル実体の交換は端末間において直接行われるために、端末間で著作権侵害となるファイル情報や、不正なウイルスファイルが配信先の端末装置に送信される危険性がある。また、ネットワークを介して端末間で勝手なデータのやり取りを行ったとしても管理装置では不正行為の防止等の管理を行うことはできない。

また、上述した電子すかしを用いた方式では、「すかし」を認証する際の端末における処理負荷が大きく、処理速度が遅くなるという問題がある。

さらに、特許文献１に示す方法では、端末自身が登録されるデータの正当性を確認するため、端末側で不正なデータを処理できるという問題がある。

またさらに、端末装置でのデータ処理において認証サーバを用いる場合においては、サーバ装置において一意にデータを管理して配信するために、認証や配信という全ての処理をサーバ装置が担うことにより、サーバ装置へのアクセス集中等による処理負担が生じている。さらに、サーバ装置においてデータの配信先端

末が認証されてしまうと、例えば有料コンテンツ配信のように会員制の閉じたネットワークではどのような情報がやり取りされたか管理できないという課題がある。

SUMMARY OF THE INVENTION

本発明は前記従来の問題点を解決することを目的とし、管理装置を用いて端末間で処理されるデータを管理する場合において、端末間及び管理装置において大きな処理負担を与えずにデータのやり取りを管理して、且つ端末間においては不正なデータ処理を防止して安全性の確認されたデータのやり取りを行うことができる管理装置及び端末装置を提供することを目的とする。

【課題を解決するための手段】

このような課題を解決するために、本発明に係る管理装置は［請求項１］、［請求項２］、より好ましくは［請求項３］。

このため、本発明に係る管理装置においては、処理を開始する端末装置からの許可依頼信号を受信して、検証手段において端末間でやり取りされるデータの正当性を当該データに基づいて検証して、検証が認められる場合には端末装置に許可信号を発行する。従って、管理装置は許可信号に基づいて端末装置間のデータのやり取りを管理できる。

また、前記検証手段は処理対象のデータの一部を用いて検証を行うために、管理装置側においては全てのデータを記録、管理する必要はなく、検証処理における負担を軽減することができる。

また、本発明に係る端末装置は、［請求項１４］、［請求項１５］、より好ましくは［請求項１７］。

このため、本発明に係る端末装置においては、他の端末装置とのデータの処理を開始しようとする場合においては、処理許可信号を生成して管理装置に送信する。また、端末装置は管理装置からデータの該当情報の返答要求がある場合には該当情報の作成を行い管理装置に返答する。さらに、端末装置においては管理装置からの処理の許可情報を受信した場合において端末装置との処理を開始できる。従って、不正なデータの処理を防止して、管理装置において安全性の確保された

データのやり取りを行うことが可能となる。

尚、本発明は、上述のような管理装置及び端末装置として実現できるのみではなく、この管理装置と端末装置とがネットワークを介して接続されてなる管理システム、この管理装置が備える手段をステップとする管理方法、当該管理方法をコンピュータ等で実現させるプログラムとして実現したり、当該プログラムをＤＶＤ、ＣＤ－ＲＯＭ等の記録媒体や通信ネットワーク等の伝送媒体を介して流通させることができるのは言うまでもない。

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects, advantages and features of the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings which illustrate a specific embodiment of the invention. In the Drawings:

図１は、実施の形態１係る端末間のデータ処理における管理システムの構成図の一例である。

図２は、実施の形態１に係る管理装置の詳細な機能ブロック図である。

図３は、実施の形態１に係る処理依頼端末の詳細な機能ブロック図を示す。

図４は、実施の形態１に係る依頼先端末の詳細な機能ブロック図を示す。

図５は、実施の形態１に係る管理システム全体におけるデータの流れの概要を説明するためのシーケンス図である。

図６は、実施の形態１に係る管理システムにおいて管理装置と処理依頼端末と依頼先端末との間で交換されるデータの構成図である。

図７は、実施の形態１に係る管理装置が処理依頼端末から配信の許可依頼信号を受信してから配信許可信号を処理依頼端末に送信するまでの動作手順を示すフローチャートである。

図８は、実施の形態１に係る処理依頼端末から管理装置に許可依頼信号が送信されてから配信依頼を発行するまでの動作手順を示すフローチャートである。

図９は、実施の形態１に係る依頼先端末が管理装置からデータ確認信号を受信してから処理依頼端末に対してファイル情報の配布を開始するまでの動作手順に

ついて示すフローチャートである。

図１０は、実施の形態１に係る管理システムにおいてコンテンツホルダーとなる依頼先端末から管理装置に作成したファイル情報をアップロードする場合の動作手順を示すフローチャートである。

図１１は、該当情報抽出部を備えた管理装置の機能ブロック図である。

図１２は、許可信号発行部及びデータ確認部の両方の機能を併せ持つ処理端末の機能ブロック図である。

図１３は、実施の形態２に係る管理システムを構成する管理装置、処理依頼端末、及び依頼先端末の機能ブロック図を示す。

図１４は、実施の形態２に係る管理装置の許可依頼を受信してから許可情報を発行するまでの動作手順を示すフローチャートである。

図１５は、データ登録部に記録されているデータの参考図である。

図１６は、実施の形態３に係る管理システムの全体図を示す。

図１７は、実施の形態３に係る管理システムにおけるデータの流れの概要を説明するためのシーケンス図である。

図１８は、実施の形態３に係る処理依頼端末が依頼先端末に対して発行する処理許可依頼信号のデータ構成の一例を示す。

図１９は、実施の形態４に係るリモートメンテナンスに用いる管理システムの全体図を示す。

図２０は、従来のネットワークを介した管理装置及び端末間におけるデータ管理の全体図を示す。

DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

以下、本発明に係る管理システムについて図面を参照して説明を行う。尚、以下の説明及び図面は例示であり、本発明はこれらに限定されることを意図しない。また、下記の実施の形態の説明においては、端末装置間での音楽ファイルや動画ファイルのコンテンツファイルの配信における処理について説明を行うが、端末間での処理は配信に限定されるものではなく、ファイル情報の移動や消去等も行うことが可能となる。

（実施の形態１）

図１は本実施の形態１係る端末間のデータ処理における管理システムの構成図の一例である。本実施の形態１に係る管理システムは、処理依頼端末１１０、依頼先端末１２０、及び処理依頼端末１１０と依頼先端末１２０と間でのやり取りされるファイル情報の管理を行う管理装置１００がネットワークバス１３０を介して相互に接続されて構成される。

端末間においてやり取りされるファイル情報の管理を行う管理装置１００は、ネットワークを介して処理依頼端末１１０及び依頼先端末１２０と通信する通信部１０１、処理依頼端末１１０から送信される処理許可依頼信号を受信する許可信号受信部１０２、データ確認部１０５での確認内容に応じて処理依頼端末１１０及び依頼先端末１２０に処理の許可信号、或いは不許可信号を送信する許可情報送信部１０３、許可信号受信部１０２で受信された処理許可依頼信号の内容を処理する許可信号処理部１０４、及び端末間で処理されるデータの内容及び正当性を確認するデータ確認部１０５を備える。

他の端末装置からのファイル情報の取得を要求して管理装置１００に対して処理依頼のための依頼信号を発行する処理依頼端末１１０は、依頼先端末１２０や管理装置１００と通信する通信部１１１、管理装置１００から発行される許可／不許可情報を受信する許可情報受信部１１２、管理装置１００に送信する配信の処理許可依頼信号を発行する許可信号発行部１１３、及び管理装置１００から許可された内容に応じてデータの処理を行うデータ処理部１１４を備える。

ファイル情報を保持している依頼先端末１２０は、処理依頼端末１１０及び管理装置１００と通信するための通信部１２１、管理装置１００から発行された許可／不許可情報を受信する許可情報受信部１２２、管理装置１００から送られてくるデータ確認信号を処理するデータ確認部１２３、及び管理装置１００からの要求に対して返答を行うデータ処理部１２４を備える。

図２は､本実施の形態１に係る管理装置１００の詳細な機能ブロック図である。

データ確認部１０５は、許可信号処理部１０４から送られてきた処理許可依頼信号の内容を確認する該当情報確認部１０５ａ、該当情報に関して管理装置１００のデータベースが保持している情報を読み出す該当情報読出し部１０５ｂ、該

当情報を有する依頼先端末１２０に該当情報の返答を要求する該当情報送信要求部１０５ｃ、送信要求に関して該当情報を有する依頼先端末１２０からの回答を受信する該当情報受信部１０５ｄ、管理装置１００側で保持している該当情報と依頼先端末１２０からの回答に含まれる該当情報とを比較する該当情報比較部１０５ｅを備える。

次に、図３に本実施の形態１に係る処理依頼端末１１０の詳細な機能ブロック図を示す。

データ処理部１１４は、管理装置１００から返答される許可情報内容からＣＰＵ等の処理実行部に適切な処理命令を生成する処理命令生成部１１４ａ、キーボード等のユーザインタフェースから入力される処理に関するコマンドを受け付ける処理命令受付部１１４ｂ、及びユーザインタフェースから入力されたコマンドの内容を確認する処理命令確認部１１４ｃを備える。この処理命令受付部１１４ｂにおいて受け付けられる情報は、例えば、特定の動画ファイルの配信要求である。

図４は、本実施の形態１に係る依頼先端末１２０の詳細な機能ブロック図を示す。

データ処理部１２４は、管理装置からの要求に従って処理対象となっているファイル情報から該当情報を読み出す該当情報読出し部１２４ａ、管理装置１００から送信される処理許可情報に基づいて処理命令を生成する処理命令生成部１２４ｂとを備える。

該当情報読出し部１２４ａは、データ確認部１２３から処理データを受け取ると、指定されたファイル及び指定箇所を確認してメモリ等のデータ格納部からデータを読み出す。

処理命令生成部１２４ｂは、許可情報受信部１２２から配信の許可信号を受け取ったら、処理依頼端末１１０との間のファイル情報の配信を処理受付開始状態になるようにＣＰＵ等の処理実行部に送信する。また、処理命令生成部１２４ｂは、許可情報受信部１２２が不許可信号を受け取った場合には、処理依頼端末１１０からの処理を受け付けないような命令を生成する。

以上のように構成された本実施の形態１に係る管理システムの動作手順につい

ての図５から図９を用いて説明を行う。

図５は、本実施の形態１に係る管理システム全体におけるデータの流れの概要を説明するためのシーケンス図である。尚、管理装置１００は、データ確認部１０５の該当情報比較部１０５ｅにおいてファイル情報の正当性を比較するため、予め端末間でやり取りされるファイル情報をダウンロード等により取得してデータベースに登録（５０１）する。そして、本実施の形態１に係る管理装置１００は端末装置間でやり取りされるファイル情報の全体を登録するのではなく、少なくとも一部を抽出してデータベースに登録することを特徴とする。

最初に、処理依頼端末１１０は、依頼先端末１２０からファイル情報の取得を要求する際には、許可信号発行部１１３は、管理装置１００に処理許可依頼信号を送信する（５０２）。

次に、処理許可依頼信号を受信した管理装置１００は、やり取りされるファイル情報の正当性を確認するために、該当情報送信要求部１０５ｃから依頼先端末１２０に対して該当情報の返信要求（５０３）の送信を行う。この該当情報としては、やり取りされるファイル情報の特定位置の値等である。

そして、管理装置１００から該当情報返答要求（５０３）を受信した依頼先端末１２０は、該当情報読出し部１２４ａにおいて保持しているファイル情報から該当情報を読み出して、通信部１２１を介して管理装置１００側に該当情報（５０４）の返答を行う。

また、管理装置１００の該当情報受信部１０５ｄにおいて受信された該当情報は、該当情報比較部１０５ｅにおいて同一性の判断が行われ、配信先端末１２０の有しているファイル情報に正当性があるか否かの判定を行う。

そして、管理装置１００において管理されている該当情報と配信先端末から返答された該当情報とが一致して正当性が認証された場合においては、管理装置１００から配信許可信号（５０５及び５０６）が処理依頼端末１１０及び依頼先端末１２０に送信される。

次に、配信許可信号（５０５）を受信した処理依頼端末１１０は、依頼先端末１２０に直接ファイル情報の配信依頼（５０７）を行い、配信依頼（５０７）を受信した依頼先端末１２０は、配信許可信号（５０６）に記載されている処理に

基づいて要求のあるファイル情報のデータ配信（５０８）を処理依頼端末１１０に送信して、一連の配信処理を終了する。

図６は、本実施の形態１に係る管理システムにおいて管理装置１００と処理依頼端末１１０と依頼先端末１２０との間で交換されるデータの構成図である。

図６（ａ）は、処理依頼端末１１０の許可信号発行部１１３で生成され管理装置１００に送信される処理許可依頼信号６００のデータ構成の一例を示す。この処理許可依頼信号６００は、送信先及び送信元のアドレス情報を記載するヘッダ部６０１、及び処理許可依頼信号を発行する処理依頼端末１１０のユーザＩＤ６０３、依頼先端末１２０の処理相手ユーザＩＤ６０４、処理対象となるファイル名を表す処理対象ファイル番号６０５、管理装置１００に許可を依頼する処理の種別を表す処理種別番号６０６を含むデータ部６０２より構成される。尚、処理種別番号６０６に記載される処理の種別とは、例えば配信、消去、移動等である。

図６（ｂ）は、管理装置１００の該当情報返信要求部１０５ｃにおいて生成され依頼先端末１２０に送信される該当情報返信要求６１０のデータ構成を示す図である。この該当情報返信要求６１０には、ヘッダ部６１１にアドレス情報、データ部６１２には処理対象ファイル番号６１３及び返答を要求する要求情報６１４が記述されている。依頼先端末１２０の該当情報読出し部１２４ａにおいては、この要求情報６１４に従ってやり取りされるファイル情報の該当箇所のデータを読み込み、該当情報を含んだ返信パケット６２０を生成して管理装置２００に送信する。

図６（ｃ）は、依頼先端末１２０のデータ処理部１２４で生成され管理装置１００に該当情報を返信するための返信パケット６２０のデータ構成の一例を示す。この返信パケット６２０は、アドレス情報を含むヘッダ部６２１、及び処理対象ファイル番号６２３や該当情報６２４を含むデータ部６２２より構成される。

図７は、本実施の形態１に係る管理装置１００が処理依頼端末１１０から配信の許可依頼信号を受信してから配信許可信号を処理依頼端末１１０に送信するまでの動作手順を示すフローチャートである。

最初に、管理装置１００における処理許可確認動作について説明を行う。管理装置１００において許可信号受信部１０２は、通信部１０１経由で処理依頼端末

１１０から処理許可依頼信号を受信すると（Ｓ７０１）、許可信号処理部１０４は許可依頼信号６００に記述されているユーザＩＤ６０３を用いて処理依頼端末１１０の確認を行う（Ｓ７０２）。

また、許可信号処理部１０４は、配信要求のあるファイル情報を保持する依頼先端末１２０を処理相手ユーザＩＤ６０４より取得して確認を行い（Ｓ７０３）、また、処理対象ファイル番号６０５及び処理種別番号６０６を読み出して処理許可依頼信号の内容を解析する（Ｓ７０４及びＳ７０５）。ここで、例えば、処理種別番号６０６は「配信」を表す「０」である。尚、例えば、ファイルの移動の場合には、処理種別番号６０６では「移動」を表す「２」が多重され、処理依頼端末１１０が依頼先端末１２０が保存しているファイルの「消去」の許可を依頼する場合には、処理種別番号６０６では消去を表す「１」が多重される。

そして、許可信号処理部１０４は、該当ファイルデータの読出しを行い（Ｓ７０６）、ファイル情報の端末間での配信許可を与える可能性があると判断した場合には、データ確認部１０５に処理を依頼する。データ確認部１０５においては、許可信号処理部１０４より送られてきた処理許可依頼信号の内容を該当情報確認部１０５ａで確認する。

次に、該当情報確認部１０５ａは、処理許可依頼信号から該当ファイルを持っている依頼先端末１２０及び該当ファイルを確認し、該当情報読出し部１０５ｂは、該当情報確認部１０５ａで確認された該当ファイルに関する情報をデータベースより読み出す。

また、該当情報送信要求部１０５ｃでは該当ファイルを持っている依頼先端末１２０に、ファイルの正当性を確認するために必要な情報の返答要求を行うための該当情報返信要求６１０を生成して依頼先端末１２０に送信する（Ｓ７０７）。

次に、該当情報受信部１０５ｄでは、要求に対して依頼先端末１２０から返答された該当情報を受信する処理を行う（Ｓ７０８）。そして、受信した場合には該当情報比較部１０５ｅへ送る。該当情報比較部１０５ｅでは、依頼先端末１２０から送られてきた情報と該当情報読出し部１０５ｂで読み出した情報を比較し、同一性が確認されて正当なデータであると判断したら（Ｓ７０８でＹ）、認証のためにこの確認処理を数箇所に渡って比較処理をＮ回行うか否かの判定を行う（Ｓ

７０９)。尚、この該当情報比較部１０５ｅにおける端末間でのファイル情報の検証処理の一例としては、ファイルの指定位置の値を返答、ファイルのヘッダ等、特定フォーマット部を送信させ、例えば暗号化フラグが立っているか等を確認する方法である。

そして、該当情報比較部１０５ｅはＮ回の判定処理を終了すると（Ｓ７０９でＹ)、端末間でのデータの処理の許可を示す許可情報を許可情報送信部１０３に送信する。一方、該当情報比較部１０５ｅは、正当なデータでないと確認した場合には（Ｓ７０８でＮ)、端末間での処理の不許可を示す処理不許可情報を許可情報送信部１０３に送信する。

許可情報送信部１０３では、許可信号処理部１０４又はデータ確認部１０５から送られてきた処理許可情報或いは処理不許可情報を、通信部１０１を介して処理依頼端末１１０及び依頼先端末１２０に送信する(Ｓ７１０及びＳ７１１)。尚、図７においては、Ｓ７１１の処理不許可情報の発行を行ったが、これは必ずしも行う必要はなく、この手順を省略することも可能である。

続いて、処理許可依頼信号を発行する処理依頼端末１１０における動作について説明を行う。図８は、本実施の形態１に係る処理依頼端末１１０から管理装置１００に許可依頼信号が送信されてから配信依頼を発行するまでの動作手順を示すフローチャートである。

最初に、データ処理部１１４の処理命令受付部１１４ｂよりキーボード等のユーザーインターフェースを用いて配信を要求するファイル情報や処理内容を指定して、許可信号発行部１１３に対して許可信号の発行の入力を行うと(Ｓ８０１)、処理命令受付部１１４ｂは、入力された情報を受付けて処理命令確認部１１４ｃへ送信する。

次に、処理命令確認部１１４ｃでは受け付けられた情報のうち、管理装置１００へ許可を求める必要がある命令を抽出し、許可を依頼する処理内容を許可信号発行部１１３へ送信する。

そして、許可信号発行部１１３は、管理装置１００へ送信するための処理許可依頼信号を発行して（Ｓ８０２)、通信部１１１を介して管理装置１００に送信する。

次に、許可信号発行部１１３が処理許可依頼信号を発行して管理装置１００に送信した場合においては、許可情報受信部１１２は、管理装置１００から送られてくる許可情報或いは不許可情報の受信処理を行う（Ｓ８０３）。

そして、管理装置１００におけるやり取りされるデータの正当性の検証が行われ、許可情報受信部１１２が配信許可情報を受け取った場合には（Ｓ８０３でＹ）、データ処理部１１４に送信する。一方、配信許可信号を受信しない場合にはＳ８０１における再度配信許可依頼信号の入力処理を行う（Ｓ８０３でＮ）。

そして、データ処理部１１４の処理命令生成部１１４ａは、許可情報受信部１１２から送られてきた許可情報を解析する（Ｓ８０４）。この場合、処理命令生成部１１４ａは、不許可の場合においては（Ｓ８０４でＮ）、配信不許信号の発行を行い（Ｓ８０６）、許可の場合においては（Ｓ８０４でＹ）、許可内容に応じた配信依頼信号を生成して（Ｓ８０５）、依頼先端末１２０に送信して一連の処理を終了する。

次に、本実施の形態１に係る依頼先端末１２０が管理装置１００からデータ確認信号を受信してから処理依頼端末１１０に対してファイル情報の配布を開始するまでの動作手順について、図９に示すフローチャートを用いて説明する。

まず、データ処理部１２４の該当情報読出し部１２４ａは、管理装置１００からデータ確認信号を受信すると（Ｓ９０１）、指示されたファイル情報の指示された位置の値を読み出し該当情報として返信パケット６２０を生成して管理装置１００に返信する（Ｓ９０２）。

次に、依頼先端末１２０の許可情報受信部１２２は、管理装置１００から配信許可情報の受信処理を行う（Ｓ９０３）。この受信処理を行った場合においては（Ｓ９０３でＹ）、データ確認部１２３は管理装置１００からの要求されるファイル情報の配信の許可／不許可の判定を行う（Ｓ９０４）。尚、許可情報受信部１２２は受信処理を行わない場合においては（Ｓ９０３でＮ）、再度Ｓ９０１からのデータ確認信号受信処理を行う。

データ確認部１２３は、配信許可であると判定する場合においては（Ｓ９０４でＹ）、処理依頼端末１１０からの配信受付状態として処理依頼端末１１０からの配信受付を開始して（Ｓ９０５）、不許可である場合においては（Ｓ９０４でＮ）、

配信不許可信号を生成して処理依頼端末１１０からの配信要請を受け付けない（Ｓ９０６）。以上により一連の依頼先端末１２０における処理を終了する。

図１０は、本実施の形態１に係る管理システムにおいてコンテンツホルダーとなる依頼先端末１２０から管理装置１００に作成したファイル情報をアップロードする場合の動作手順を示すフローチャートである。

最初に、コンテンツの作成又は取得を行う依頼先端末１２０は、管理装置１００に対してファイル情報のアップロードを行う（Ｓ１００１）。このファイル情報は図１１に示すように依頼先端末１２０のファイル作成部１１０２において作成される、例えば音楽ファイルや動画ファイルとなる。また、ファイル情報は他の端末装置から購入したファイル情報でも構わない。

管理装置１００のデータ確認部１０５は、送信されたファイル情報の内容を確認して、管理するためのファイル情報の一部を抽出して（Ｓ１００２）、抽出された情報をデータベースに格納する（Ｓ１００３）。この情報の抽出方法としては、例えば、図１１に示すように、管理装置１００のデータ確認部１０５に該当情報抽出部１１０１を備えることにより実現される

以上の説明のように、本実施の形態１に係る管理装置１００は、端末間での配信を依頼する処理依頼端末１１０から送信される処理許可信号を受信する許可信号受信部１０２、依頼先端末１２０に対して配信要求のあるファイル情報の特定位置の情報の返答を要求する該当情報送信要求部１０５ｃ、端末装置間でやり取りされるデータの一部を抽出して保持する該当情報抽出部１１０１、抽出されてデータベースに記録されているファイル情報と依頼先端末１２０から返答される返答パケットに含まれる該当情報の比較を行い端末間でやり取りされるファイル情報の正当性を検討する該当情報比較部１０５ｅを備える。

また、本実施の形態１に係る処理依頼端末１１０は、管理装置１００に対して許可依頼信号の発行を行う許可依頼発行部１１３、管理装置１００より許可信号を受信した場合において他の端末装置との間の処理命令を生成する処理命令生成部１１４ａを備える。

さらに、依頼先端末１２０は、管理装置１００から配信対象のファイルの該当情報の読出しを行うと共に、返信パケット６２０の生成を行う該当情報読出し部

１２４ａ、管理装置１００から配信許可信号を受信して他の端末装置との間の処理命令の生成を行う処理命令生成部１２４ｂを備える。

従って、端末間でファイル情報のやり取りを行う際には、処理依頼端末１１０はまず管理装置１００に対して処理依頼信号を送信し、管理装置１００の該当情報比較部１０５ｅにおいて配信対象のファイル情報の正当性を確認して、管理装置１００が配信許可情報を処理依頼端末１１０及び依頼先端末１２０に送信した後において、端末間での正規のやり取りを開始できる。このため、端末装置間において不正なファイル情報の配信を防止して、安全性を保証した管理システムとすることが可能となる。

また、管理装置１００における端末間でやり取りされるファイル情報の管理においては、配信対象のファイルを全て管理するのではなく、少なくとも一部のデータ情報を抽出して認証処理を行うために、管理装置における処理負荷を確実に軽減して、従来のサーバ装置のようにコンテンツの内容全てを記録、管理する手間を省くことができる。また、管理装置１００はやり取りされるファイルの正当性を常にチェックするため、端末装置に特別なファイル情報の検証のための領域を設ける必要がなく、処理依頼端末１１０及び依頼先端末１２０のリソースや負荷を軽減しつつネットワークの信頼性を高める効果がある。

そして、管理装置１００においては、端末間のファイル情報の配信においては、ファイル情報の実体でなく、許可信号のやり取りが行われるのみなので、大容量のコンテンツファイルの送受信や管理を行う必要がなく、管理装置１００における処理を大きく軽減できると共に、端末間で安全なファイル情報の交換が行える。

また、依頼先端末１２０は管理装置１００にファイル情報を登録することにより、各自で安全性のあるファイル情報のやり取りを各自でネットワークを介した他の端末装置と行えるようになるため、勝手にファイル情報をコピーされることを防止して、利用者は安心してファイル交換を行うことが可能となる。

さらに、処理情報の名前を管理装置側のデータベースに登録して、正規に登録されたファイル以外の処理を認めないことにより、端末間でやり取りされるネットワークの安全性を向上させる効果がある。

また、処理情報の内容を管理装置１００側のデータベースに登録して処理情報

の内容確認に用いることにより、処理情報の正当性を高める効果がある。

尚、図１２に示すように、処理端末１２００は、許可信号の発行を行う許可信号発行部１１３、及び該当情報の返答を行うデータ確認部１２３の両方の機能を併せ持つことも考え得る。

このように、処理端末１２００が処理を依頼する構成と処理を依頼される構成の両方を搭載することにより、例えば処理依頼端末としてコンテンツホルダー等の端末装置からファイル情報の配信を受けた処理端末１２００は、管理装置１００の許可の元、今度は処理を依頼される側の端末として、処理を依頼する側の端末装置に対して以前に受信したファイル情報を配信することが可能となる。

尚、配信処理を行う際、本実施の形態１では配信許可が出ると、処理依頼端末１１０から依頼先端末１２０にアクセスしていたが、管理装置１００から依頼先端末１２０に発行する許可情報に相手先情報を多重して、依頼先端末１２０からファイル情報の配信作業を開始することも可能である。

また、本発明に係る管理装置１００は、コンテンツファイル等のファイル情報を保持する依頼先端末１２０の側から、ファイル情報を送信するための配信依頼を受信して、管理装置１００を介して他の端末装置に正当性の検証されたファイル情報の配信を行うことも可能となる。このため、本発明に係る管理システムは、コンテンツファイルの作成を行う側の端末装置が作成したコンテンツファイルを配信したいような場合においても有効となる。

（実施の形態２）

次に、本発明に係る実施の形態２についての説明を行う。

本実施の形態２に係る管理装置１００は、依頼先端末１２０よりアップロードされるファイル情報の少なくとも一部を記録するデータ登録部１３０１を備えることを特徴とする。尚、上述した実施の形態１に係る管理装置１００、処理依頼端末１１０、及び依頼先端末１２０と同じ構成においては同様の符号を付し詳細な説明は省略する。

図１３は、本実施の形態２に係る管理システムを構成する管理装置１００、処理依頼端末１１０、及び依頼先端末１２０の機能ブロック図を示す。本実施の形態２においては、管理装置１００がデータ登録部１３０１を備える。

データ登録部１３０１には、依頼先端末１２０からアップロードされたファイル情報の内容の一部が記録されている。管理装置１００は、データ登録部１３０１に記載されている限り対象の依頼先端末１２０に対するファイル情報の確認処理を行う。そして、データ登録部１３０１にはファイル情報の名前だけでなくデータ自体を登録することにより、管理装置１００におけるデータの確認精度を向上させることができる。

次に、本実施の形態２に係る管理装置１００の動作手順について説明する。

図１４は、本実施の形態２に係る管理装置１００の許可依頼を受信してから許可情報を発行するまでの動作手順を示すフローチャートである。尚、本実施の形態２においては、管理装置１００が配信許可依頼信号から読み出されたファイル情報がデータ登録部１３０１に登録されたファイル情報として存在するかを確認する処理（Ｓ１４０７）を行うことを特徴とする。

最初に、管理装置１００において許可信号受信部１０２は、処理許可依頼信号を受信すると（Ｓ１４０１）、許可信号処理部１０４は許可依頼信号６００に記述されているユーザＩＤ６０３を用いて処理依頼端末１１０の確認し（Ｓ１４０２）、配信要求のあるファイル情報を保持する依頼先端末１２０を処理相手ユーザＩＤ６０４より取得して確認を行い（Ｓ１４０３）、また、処理対象ファイル番号６０５及び処理種別番号６０６を読み出して処理許可依頼信号の内容を解析する（Ｓ１４０４及びＳ１４０５）。

次に、許可信号処理部１０４は、該当ファイルデータの読出しを行い（Ｓ１４０６）、本実施の形態２に係る管理装置１００が配信許可依頼信号から読み出されたファイル名がデータ登録部１３０１に登録されたファイル情報として存在するかを確認する処理（Ｓ１４０７）を行う。この確認処理により、データ登録部１３０１に登録されていないファイルである場合においては（Ｓ１４０７でＮ）、許可発行不可となり配信不許可信号が依頼先端末１２０に発行される（Ｓ１４１２）。

一方、データ登録部１３０１に登録されているファイル情報である場合においては（Ｓ１４０７でＹ）、該当情報確認部１０５ａは、処理許可依頼信号から該当ファイルを持っている依頼先端末１２０及び該当ファイルを確認し、該当情報読出し部１０５ｂは、該当情報確認部１０５ａで確認された該当ファイルに関する

情報をデータ登録部１３０１より読み出す。

また、該当情報送信要求部１０５ｃでは該当ファイルを持っている依頼先端末１２０に、データ確認のための該当情報返信要求６１０を生成して依頼先端末１２０に送信する（Ｓ１４０８）。次に、該当情報受信部１０５ｄでは、要求に対して依頼先端末１２０から返答された該当情報を受信する処理を行う（Ｓ１４０９）。そして、受信した場合には該当情報比較部１０５ｅへ送る。該当情報比較部１０５ｅでは、依頼先端末１２０から送られてきた該当情報とデータ登録部１３０１より該当情報読出し部１０５ｂで読み出した該当情報を比較し、同一性が確認されて正当なデータであると判断したら（Ｓ１４０９でＹ）、認証のためにこの確認処理を数箇所に渡って比較処理をＮ回行うか否かの判定を行う（Ｓ１４１０）。

そして、該当情報比較部１０５ｅは、Ｎ回の判定処理を終了すると（Ｓ１４１０でＹ）、処理許可情報を許可情報送信部１０３に送信する。一方、該当情報比較部１０５ｅは、正当なデータでないと確認した場合には（Ｓ１４０９でＮ）、処理不許可情報を許可情報送信部１０３に送信する。

許可情報送信部１０３では、許可信号処理部１０４又はデータ確認部１０５から送られてきた処理許可情報或いは処理不許可情報を、通信部１０１を介して処理依頼端末１１０及び依頼先端末１２０に送信する（Ｓ１４１１及びＳ１４１２）。

尚、データ登録部１３０１でデータと共に端末情報も登録し、図１４の許可発行可能ステップ（Ｓ１４０７）でファイルの内容だけでなく、端末ごとに許可不許可条件をつけることも可能である。

図１５は、データ登録部１３０１に記録されているデータの参考図である。

最初に、データ確認部１０５における端末間でやり取りされるデータの正当性を確認する方法として、依頼先端末１２０に配信対象のファイルのアドレスを指定して、依頼先端末１２０のデータ確認部１２３にその箇所の値を返答させるようにする。

例えば、管理装置１００の該当情報送信要求部１０５ｃからアドレス「０ｘ００００」の位置の値の返答要求が依頼先端末１２０に対して発行されると、依頼先端末１２０の該当情報読出し部１２４ａは指定された位置のデータを読み出してその値を返す。

該当情報比較部１０５ｅでは、返答された値を「0010（１５０１に記載)」とデータ登録部１３０１に記録されている値と比較し、同一であることが確認できれば、次にファイル情報の数箇所のアドレス「０ｘ０００４」、アドレス「０ｘ０１１６」、アドレス「０ｘＡＡＦＥ」の値の返答を要求し、それぞれ「1010（１５０２に記載)」、「１１１０（１５０３に記載)」、「０１１１（１５０４に記載)」と同一であることが確認できれば、端末間でやり取りされるデータファイルが正規なものであると判断できる。

尚、本発明における管理装置１００のデータ確認部１０５の確認においては、データ登録部１３０１にはファイル全部を登録する必要はなく、データの正当性確認用に適当なアドレスとそこに本来書かれているべき値をいくつかセットで保持してメモリ資源と節約しつつ同等の効果が得られる。また、同じファイルであっても端末毎やアクセス時毎に指定する箇所を変更することによって、管理装置１００において、より高いファイル情報の正当性を確保できる。

また、該当情報比較部１０５ｅにおける配信対象のファイル情報の正当性の確認の方法としては、依頼先端末１２０に対して指定されたデータパターンがファイルのどの位置に多重されているかを返答させたり、指定されたデータパターンがファイル内に何箇所で多重されているかを返答させたりする方法も考え得る。

さらに、過去の処理履歴を管理装置１００側で管理して、過去の処理履歴の内容に応じてデータの確認方法を変更することも考え得る。例えば管理装置１００において、過去数十回連続で正しい処理を行った端末装置における検証処理を軽減して簡素化したり、過去に不正を行ったことのある端末装置の検証処理の回数や種類を増やすことにより端末間でやり取りされるファイル配信における処理効率を高めたり、安全性を確保することも可能である。

以上のように、本実施の形態２に係る管理システムにおいては、管理装置１００が端末間でやり取りされるファイル情報を記録、管理するデータ登録部１３０１を保持する。

従って、管理装置１００が管理する端末装置間でのデータのやり取りは、データ登録部１３０１に登録された情報のみ配信許可が可能となり、ネットワーク上での不正なファイル情報の配信を防止できる。また、データ登録部１３０１には

配信されるファイル情報の少なくとも一部が登録されるため、動画等の大容量のファイル情報の全てを管理する必要性はなく、管理装置１００におけるデータ管理を容易化することができる。

また、上述の実施の形態２においてデータ登録部１３０１に登録可能なデータフォーマットを暗号化ファイルと規定してファイルが正しく配布された場合に暗号を解除する鍵を配布することにより、ネットワークのセキュリティを高めることが可能となる。

そして、この暗号化ファイルであるかの確認方法の一例としては、ファイルの形式がＭＰＥＧ２　ＳＹＳＴＥＭＳ規格で規定されたトランスポートストリームであれば、トランスポートストリームパケットのヘッダ部に多重されているｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌビット（先頭から２５ビット目及び２６ビット目）を確認する方法がある。

もちろん、暗号化ファイルを管理装置１００に登録してファイルの内容をチェックすることによってもさらにセキュリティを高めることが可能である。尚、鍵の配布は管理装置１００が行っても良いし、また他の例えば鍵管理を行う鍵サーバが行っても良い。

（実施の形態３）

次に、実施の形態３について説明を行う。本実施の形態３に係る管理システムは、処理依頼端末１１０から管理装置１００に配信許可依頼を行うのではなく、依頼先端末１２０に依頼先端末１２０に直接配信依頼を行い、管理装置１００と依頼先端末１２０との間でデータの検証を行う。

図１６は、本実施の形態３に係る管理システムの全体図を示す。

本実施の形態３において上述の実施の形態１と異なる点は、処理を依頼される依頼先端末１６００が許可信号発行のための許可信号発行部１６０１を備える点である。

次に、本実施の形態３に係る管理システムの動作手順について図１７を参照して説明する。図１７は、本実施の形態３に係る管理システムにおけるデータの流れの概要を説明するためのシーケンス図である。尚、管理装置１００は、予めファイル情報の配信を行う依頼先端末１６００からファイル情報を取得して少なく

とも一部の情報を抽出してデータ登録部１３０１に登録（１７０１）している。

最初に、処理依頼端末１１０の許可信号発行部１１３は処理許可依頼信号を発行して、依頼先端末１６００に通信部１１１を介して配信依頼（１７０２）を行う。

そして、依頼先端末１６００は、処理依頼端末１１０からの処理許可依頼信号を受け取ると、許可信号発行部１６０１は処理許可依頼信号（１７０３）を管理装置１００に送る。但し、処理許可依頼信号に含まれるユーザＩＤには依頼先端末１６００の識別番号を多重する。

管理装置１００では、依頼先端末１６００に対して該当情報返信要求（１７０４）を行い、該当情報（１７０５）を受信して許可処理依頼信号の解析を行う。但し、前述した実施の形態１及び２のように、依頼先端末１６００は処理許可依頼信号に多重されていないので依頼先端末確認の処理は省略される。

そして、管理装置１００でのデータ確認処理完了後、管理装置１００から発行される許可信号は依頼先端末１６００のみに送信（１７０６）される。依頼先端末１６００は、許可情報を許可情報受信部１２２で受信したら、通信部１２１を介して処理依頼端末１１０に許可情報（１７０７）を送信する。これにより処理依頼端末１１０と依頼先端末１６００との間で配信等の処理を開始することが可能となる。

最後に、依頼先端末１６００は処理依頼端末１１０に対して要求されたファイル情報等のデータ配信（１７０８）を行い、本実施の形態３に係る一連の処理を終了する。

図１８は、本実施の形態３に係る処理依頼端末１１０が依頼先端末１６００に対して発行する処理許可依頼信号１８００のデータ構成の一例を示す。この処理許可依頼信号１８００は、ヘッダ部１８０１、ユーザＩＤ１８０３、処理対象ファイル番号１８０４、処理種別番号１８０５を含むデータ部１８０２より構成され、上述の実施の形態１に係る処理許可依頼信号６００と異なる点は、処理依頼先である依頼先端末１６００に直接送信するため、処理相手ユーザＩＤ６０４が記述されていない点である。

以上の説明のように、本実施の形態３に係る管理システムにおいては、処理依

頼端末１１０から依頼先端末１６００に直接､処理許可依頼信号の送信が行われ、また、依頼先端末１６００から管理装置１００にファイルの処理依頼信号の送信が行われる。そして、管理装置１００において配信許可がされると依頼先端末１６００から処理依頼端末１１０に対して許可情報が送信される。従って、本実施の形態３に係る管理システムにおいては、様々な通信形態に応じた管理システムとして端末間のファイル情報のやり取りの正当性の管理を行うことが可能となる。

（実施の形態４）

以下、実施の形態４に係る管理システムについて説明する。

近年、ネットワークを介して家電機器を遠隔で診断したり、ＤＶＤ等の機器をバージョンアップするリモートメンテナンスが盛んに行われてきている。一方、ユーザ宅においては、受信するリモートメンテナンスデータの正当性において不安があるという問題がある。本実施の形態４においては、安全性の高いリモートメンテナンスデータをユーザ宅の修理対象の機器に送信できる管理システムを提供する。

本実施の形態４では、処理を依頼する端末と、処理を依頼される端末は異なる機器とある。そして、これらを組み合わせてネットワークを利用して家庭内の家電機器の保守や修理などを電器店等が行う家電機器等のリモートメンテナンスを実施する場合の例を図１９を用いて説明する。

図１９は、本実施の形態４に係るリモートメンテナンスに用いる管理システムの全体図を示す。

サービスセンタ１９０１はリモートメンテナンス情報の正当性の管理を行い、電器店１９０２はユーザ宅１９０３の家電機器等に対してリモートメンテナンスデータの送信を行い、ユーザ宅１９０２はＧＷ１９０４を用いてリモートメンテナンスデータを受信すると共に、ユーザ宅１９０２内のＴＶ１９０５、ＤＶＤ１９０６、ＰＣ１９０７等の機器のメンテナンス依頼を電器店１９０２に対して行う。

ユーザ宅１９０３から依頼を受けて顧客家庭のユーザ宅１９０３の機器のリモートメンテナンスを行う電器店１９０２は、最初にサービスセンタ１９０１に処理許可依頼信号を発行する。サービスセンタ１９０１では、リモートメンテナン

スデータが正しいかを検証し、正当性が検証できれば電器店１９０２及びユーザ宅１９０３の端末、例えばネットワーク対応ＴＶ等へのリモートメンテナンスデータの送信を許可する許可情報の送信を行う。

尚、悪意の第３者端末１９０８からサービスセンタ１９０１の検証だけ行って別のウイルスデータ等を送信を防止するために、ユーザ宅１９０３のＧＷ１９０４で再度メンテナンスデータ確認依頼をサービスセンタ１９０１に送信して、確認が取れた場合にメンテナンス処理実施することで、より安全性の高いリモートメンテナンスシステムとできる。また、サービスセンタ１９０１の公開鍵等を用いてリモートメンテナンスデータを暗号化することを考え得る。

以上の説明より、本実施の形態４に係る管理システムによれば、安全性の保証されるリモートメンテナンスデータをユーザ宅１９０３に送信できる。従って、従来のリモートメンテナンスにおけるユーザ宅１９０３での不安を解消して、悪意ある第三者からの不正メンテナンスデータの送信等の「なりすまし」を装った不正アクセスを確実に防止することができる。

尚、管理装置１００ではデータ登録部１３０１にファイル名やファイルの中身と共にファイルが格納されている端末を格納したファイルの登録先リストを登録するようにしても良い。

そして、管理装置１００に、端末装置からのコンテンツファイルが配信されるごとにファイルの配信先を登録先リストに追加し、更新することによって管理装置１００が常に端末間でやり取りされるファイル情報の格納先を認識できる。

管理装置１００は、登録先リストから取得を要求するコンテンツファイルを保持している端末を検索し、処理依頼端末１１０から処理許可依頼信号を受け取ったら、登録先リストから適切な依頼先端末１２０を選択して処理依頼端末１１０に通達する。

処理依頼端末１１０は通信部１１１で依頼先端末１２０の情報を受け取ったら、後は実施の形態３のように、管理装置１００から通達された依頼先端末１２０に処理許可依頼信号を発行することにより、所望のファイルの配信を受けることが可能となる。

尚、管理装置１００は処理依頼端末１１０から処理許可依頼信号を受け取った

ら登録先リストから適切な依頼先端末１２０を選択し、後は実施の形態1と同じように、直接コンテンツファイルの依頼先端末１２０にデータ確認処理を行っても良い。

以上のように、管理装置１００が登録先リストより依頼先端末１２０を検索することにより、処理依頼端末１１０は、コンテンツホルダーである依頼先端末１２０に関する情報を知らなくてもファイル情報の安全な交換を行うことが可能となる。尚、登録先リストより依頼先端末１２０を検出する場合においては、処理許可依頼信号に処理相手ユーザＩＤ６０４を多重する必要はなく、処理相手ユーザＩＤ６０４を空欄とできる。

尚、管理装置１００が端末間でやり取りされるファイル情報を検証する際、処理を依頼される依頼先端末１２０の特定の記憶領域に記憶された情報のみを検証することにより、依頼先端末１２０では検証の処理対象となる情報は前記特定の記憶領域に記憶された情報のみとすることも考え得る。

さらに、上述の実施の形態で述べた端末装置において処理対象となるファイルを保持する特定の記憶領域（図示せず）は期待する情報の信頼性にあわせて、一般的な記憶装置、或いはアクセス制限等のセキュリティ機能が具備された記憶装置のいずれで構成されてもよい。また、特定の記憶領域は、ユーザが作成や指定をしてもよく、或いは端末装置のプログラムなどで生成されてもよい。

【発明の効果】

以上のように、本発明に係る管理装置においては、処理を開始する端末装置からの許可依頼信号を受信した場合には、端末間での処理対象となるデータの少なくとも一部を用いて検証処理を行うため、管理装置側でのデータ管理、検証における処理負担を軽減できる。

また、管理装置には前記検証により正当性が認められる場合には許可信号を、正当性が認められない場合においては不許可信号を端末装置に送信するため、端末間でのデータ処理における柔軟な管理システムを構築できる。

そして、本発明に係る処理を依頼する側の端末装置は、処理を開始する場合には、管理装置に配信許可依頼信号を送るだけの処理を行い、実際のデータの検証は管理装置及び処理を依頼される側の端末装置で行う。従って、処理を依頼する

側の端末装置に大きな負荷を与えずに正当性の検証されたデータのやり取りを他の端末装置との間で行うことが可能となる。

また､端末装置は､処理対象のデータは管理装置において常に検証されるため、端末装置内にデータの検証のための特別な領域を設けなくても不正処理を防止できるため、端末装置のリソースや処理負荷を軽減しつつネットワークを介した端末装置間でのデータのやり取りの信頼性を高める効果がある。

さらに、端末間でやり取りされる処理データの名前や内容の少なくとも一部を管理装置のデータ登録部に登録して、管理装置側において正規に登録されたファイル以外の処理を認めないことにより、ネットワークを介した端末装置間でのデータのやり取りの信頼性を高める効果がある。

またさらに、管理装置でデータの配信や移動等の許可／不許可の検証を行うため、端末装置間でのデータの履歴を管理、制御でき、ネットワークを介した端末装置間でのデータのやり取りの信頼性を高める効果がある。

What is claimed is:

【請求項１】　ネットワークを介して接続される端末装置間において処理されるデータの管理を行う管理装置であって、

処理を依頼する側の端末装置から送信され、前記データの処理を要求する依頼信号を受信する受信手段と、

前記依頼信号を受信した場合には、前記データの正当性を検証する検証手段とを備える

ことを特徴とする管理装置。

【請求項２】　前記検証手段は、前記データの少なくとも一部の情報を用いて正当性の検証を行い、

前記管理装置は、さらに、

前記検証手段において前記データの正当性が確認された場合には、前記端末装置に許可信号を発行し、前記データの正当性が確認できない場合には、前記処理を依頼する端末装置と処理を依頼される端末装置のいずれか或いは両方に不許可信号を発行する発行手段と、

前記許可信号又は前記不許可信号を前記端末装置に送信する送信手段とを備える

ことを特徴とする請求項１記載の管理装置。

【請求項３】　前記管理装置は、さらに、

端末装置間で処理される前記データを前記端末装置からダウンロードするダウンロード手段と、

前記ダウンロードした前記データ毎に少なくとも一部の情報を抽出する抽出手段と、

前記抽出手段で抽出される情報を記録する記録手段と、

前記処理を依頼される側の依頼先端末に、前記記録手段に記録されている第一情報に関連する情報の返答要求を行う返答要求手段とを備え、

前記検証手段は、前記第一情報と、前記依頼先端末から前記返答要求に応じて返答される第二情報とを比較することにより前記データの正当性の検証を行う

ことを特徴とする請求項２記載の管理装置。

【請求項４】　前記第一情報は、前記データの特定位置の値、又はフラグの有無である

ことを特徴とする請求項３記載の管理装置。

【請求項５】　前記第一情報は、前記データの特定ファイルパターンの箇所、又は個数である

ことを特徴とする請求項３記載の管理装置。

【請求項６】　前記第一情報は、前記データのヘッダ部、又は特定位置のフォーマット部である

ことを特徴とする請求項３記載の管理装置。

【請求項７】　前記記録手段は、暗号化された前記データのみが記録可能である

ことを特徴とする請求項３記載の管理装置。

【請求項８】　前記検証手段は、前記記録手段に登録済みのデータであるか否かを検証し、

前記発行手段は、既に前記記録手段に登録済みのデータである場合において、前記端末装置に前記許可信号を発行する

ことを特徴とする請求項３記載の管理装置。

【請求項９】　前記依頼信号には、少なくとも処理を依頼する側の端末装置、処理を依頼される側である依頼先端末、前記データの識別番号、及び前記データの処理の内容に関する情報のいずれかが含まれ、

前記管理装置は、さらに、

前記依頼信号の内容を処理する信号処理手段と、

前記依頼信号から前記データの処理を依頼される依頼先端末を特定する特定手段とを備える

ことを特徴とする請求項１記載の管理装置。

【請求項１０】　前記記録手段は、処理されるデータの登録先である端末装置を記載する登録先リストを保持し、

前記特定手段は、前記登録先リストを参照して、前記依頼先端末を特定する

ことを特徴とする請求項９記載の管理装置。

【請求項１１】　前記管理装置は、さらに、
前記登録先リストを更新するリスト更新手段を備える
ことを特徴とする請求項１０記載の管理装置。
【請求項１２】　前記管理装置は、さらに、
過去の処理履歴を保持する履歴保持手段と、
前記処理履歴に基づいて前記端末装置間でのデータの処理の判断を行う処理判断手段とを備え、
前記検証手段は、前記処理判断手段における判断に基づいて、前記データの正当性の検証を行う
ことを特徴とする請求項１記載の管理装置。
【請求項１３】　前記端末装置間での前記データの処理の内容は、配信、移動又は消去のいずれかである
ことを特徴とする請求項１記載の管理装置。
【請求項１４】　通信されるデータの処理を管理する管理装置とネットワークを介して接続され、当該管理装置において管理されるデータの処理を他の端末装置との間で行う端末装置であって、
前記データの処理の要求内容を受け付ける受付手段と、
前記データの処理を要求する依頼信号の発行を行う第二発行手段と、
当該依頼信号を前記管理装置に送信する第二送信手段とを備える
ことを特徴とする端末装置。
【請求項１５】　前記端末装置は、さらに、
前記データを記録する第二記録手段と、
前記管理装置から前記データの少なくとも一部に関する情報の返答要求を受信した場合には、前記データから前記返答要求の該当する該当情報を前記第二記録手段から読み出す読出し手段と、
前記読出し手段で読み出される前記該当情報を前記管理装置に返答する返答手段とを備える
ことを特徴とする請求項１４記載の端末装置。
【請求項１６】　前記該当情報は、前記データの特定位置の値、フラグの有無、

前記データの特定ファイルパターンの箇所、前記データの特定ファイルパターンの個数、前記データのヘッダ部、又は前記データのフォーマット部に関する情報のいずれかである

ことを特徴とする請求項１５記載の端末装置。

【請求項１７】　前記端末装置は、さらに、

前記管理装置から、他の端末装置との処理の許可を示す許可信号又は他の端末装置との処理の不許可を示す不許可信号を受信する第二受信手段と、

前記許可信号を受信した場合には、処理を依頼される依頼先装置との処理を開始すると判断する一方、前記不許可信号を受信した場合には、前記依頼先端末との処理を行わないと判断する判断手段と、

前記許可信号を受信した場合において、前記管理装置から許可された内容に応じて他の端末装置との前記データの処理を行うデータ処理手段とを備える

ことを特徴とする請求項１４記載の端末装置。

【請求項１８】　前記端末装置は、さらに、

前記許可信号を受信した場合には、前記データの処理の許可を示す許可情報を作成する作成手段を備え、

前記第二送信手段は、処理を依頼する側の端末装置に前記許可情報を送信する

ことを特徴とする請求項１７記載の端末装置。

【請求項１９】　前記端末装置は、さらに、

前記端末装置間で処理される前記データを前記管理装置にアップロードするアップロード手段を備える

ことを特徴とする請求項１４記載の端末装置。

【請求項２０】　前記第二受信手段は、他の端末装置から前記依頼信号を受信した場合においては、前記発行手段は新たな依頼信号を発行し、前記第二送信手段は当該依頼信号を前記管理装置に送信する

ことを特徴とする請求項１４記載の端末装置。

【請求項２１】　端末装置間で処理可能なデータを保持する端末装置は、他の端末装置に対して前記データの配信を行うための配信要求を作成して、前記管理装置に送信する配信要求手段を備える

ことを特徴とする請求項１４記載の端末装置。

【請求項２２】　前記端末装置間での前記データの処理の内容は、配信、移動又は消去のいずれかである

ことを特徴とする請求項１４記載の端末装置。

【請求項２３】　端末装置において処理されるデータの管理を行う管理装置と複数の前記端末装置とがネットワークを介して接続されてなる管理システムであって、

前記管理装置は、

処理を依頼する側の依頼端末から送信され、処理を依頼される側である依頼先端末での前記データの処理を要求する依頼信号を受信する受信手段と、

前記依頼信号を受信した場合には、前記データの正当性を検証する検証手段とを備え、

前記端末装置は、

前記データの処理の要求内容を受け付ける受付手段と、

前記データの処理を要求する依頼信号の発行を行う第二発行手段と、

当該依頼信号を前記管理装置に送信する第二送信手段とを備え、

前記端末装置間においては前記検証手段で検証されたデータのみ処理を行うことが可能である

ことを特徴とする管理システム。

【請求項２４】　前記管理装置は、さらに、

端末装置間で処理される前記データを前記端末装置からダウンロードするダウンロード手段と、

前記ダウンロードした前記データ毎に少なくとも一部の情報を抽出する抽出手段と、

前記抽出手段で抽出される情報を記録する記録手段と、

前記処理を依頼される側の依頼先端末に、前記記録手段に記録されている第一情報に関連する情報の返答要求を行う返答要求手段とを備え、

前記端末装置は、さらに、

前記データを記録する第二記録手段と、

前記管理装置から前記返答要求を受信した場合には、前記データから前記返答要求に該当する第二情報を前記第二記録手段から読み出す読出し手段と、

前記読出し手段で読み出される前記第二情報を前記管理装置に返答する返答手段とを備え、

前記検証手段は、前記第一情報と、前記返答手段から返答される前記第二情報とを比較することにより前記データの正当性の検証を行う

ことを特徴とする請求項２３記載の管理システム。

【請求項２５】　前記第一情報又は前記第二情報は、前記データの特定位置の値、フラグの有無、前記データの特定ファイルパターンの箇所、前記データの特定ファイルパターンの個数、前記データのヘッダ部、又は前記データのフォーマット部に関する情報のいずれかである

ことを特徴とする請求項２４記載の管理システム。

【請求項２６】　前記管理装置は、さらに、

前記検証手段において前記データの正当性が確認された場合には、前記端末装置に許可信号を発行し、前記データの正当性が確認できない場合には、前記処理を依頼する端末装置と処理を依頼される端末装置のいずれか或いは両方に不許可信号を発行する発行手段と、

前記許可信号又は前記不許可信号を前記端末装置に送信する送信手段を備え、

前記端末装置は、さらに、

前記管理装置から、前記許可信号又は前記不許可信号を受信する第二受信手段と、

前記許可信号を受信した場合には、処理を依頼される依頼先装置との処理を開始すると判断する一方、前記不許可信号を受信した場合には、前記依頼先端末との処理を行わないと判断する判断手段と、

前記許可信号を受信した場合において、前記管理装置から許可された内容に応じて他の端末装置との前記データの処理を行うデータ処理手段とを備える

ことを特徴とする請求項２３記載の管理システム。

【請求項２７】　前記データは、前記管理装置からユーザ宅の端末機器の修理をネットワークを介して行うためのリモートメンテナンスデータである

ことを特徴とする請求項２３記載の管理システム。

【請求項２８】　ネットワークを介して端末装置間において処理されるデータの管理を行う管理方法であって、

処理を依頼する側の端末装置から送信され、前記データの処理を要求する依頼信号を受信する受信ステップと、

前記依頼信号を受信した場合には、前記データの正当性を検証する検証ステップとを含む

ことを特徴とする管理方法。

【請求項２９】　前記検証ステップにおいては、前記データの少なくとも一部の情報を用いて正当性の検証を行い、

前記管理方法は、さらに、

前記検証ステップにおいて前記データの正当性が確認された場合には、前記端末装置に許可信号を発行し、前記データの正当性が確認できない場合には、前記処理を依頼する端末装置と処理を依頼される端末装置のいずれか或いは両方に不許可信号を発行する発行ステップと、

前記許可信号又は前記不許可信号を前記端末装置に送信する送信ステップとを含む

ことを特徴とする請求項２８記載の管理方法。

【請求項３０】　さらに、端末装置間で処理される前記データを前記端末装置からダウンロードするダウンロードステップと、

前記ダウンロードした前記データ毎に少なくとも一部の情報を抽出する抽出ステップと、

前記抽出ステップで抽出される情報を記録する記録ステップと、

前記処理を依頼される側の依頼先端末に、前記記録ステップにおいて記録される第一情報に関連する情報の返答要求を行う返答要求ステップとを含み、

前記検証ステップにおいては、前記第一情報と、前記依頼先端末から前記返答要求に応じて返答される第二情報とを比較することにより前記データの正当性の検証を行う

ことを特徴とする請求項２８記載の管理方法。

【請求項３１】　端末間のデータの処理を管理する管理装置のためのプログラムであって、請求項1から１３のいずれか1項に記載の管理装置が備える全ての手段をコンピュータや携帯端末に実行させる

ことを特徴とするプログラム。

【請求項３２】　他の端末装置との間でデータの処理を行う端末装置のためのプログラムであって、請求項１４から２２のいずれか1項に記載の端末装置が備える全ての手段をコンピュータや携帯端末に実行させる

ことを特徴とするプログラム。

ABSTRACT OF THE DISCLOSURES

本発明に係る管理システムは、他の端末装置からのファイル情報の取得を要求して管理装置（１００）に対して処理依頼のための依頼信号を発行する処理依頼端末（１１０）、ファイル情報を保持している依頼先端末（１２０）、及び処理依頼端末（１１０）と依頼先端末（１２０）と間でのやり取りされるファイル情報の管理を行う管理装置（１００）がネットワークバス（１３０）を介して相互に接続されて構成される。